WHAT IS CLAIMED IS:

1. A system for a secure legacy enclave in a Public Key Infrastructure (PKI) comprising:

at least one legacy server, the at least one legacy server containing at least one legacy application;

at least one client platform operatively connected to a network, the at least one client platform containing legacy client software employable by at least one user to access the at one legacy application;

a directory operably connected to the network, the directory containing information on the at least one user, the directory further containing information on each at least one user designating whether each at least one user is authorized to access the at least one legacy server; and

a Virtual Private Network (VPN) extranet gateway, the VPN extranet gateway operatively connected between the at least one legacy server and the network, the VPN extranet gateway requesting a signature certificate of the at least one user attempting access to the legacy application to authenticate the at least one user, the VPN extranet gateway querying the directory to confirm the at least one user is allowed access to the legacy server after authenticating the at least one user, the VPN extranet gateway establishing a connection between the legacy client software and the legacy application if the at least one user is allowed access to the legacy server.

2. The system according to claim 1, wherein the directory comprises a database.

3. The system according to claim 1, further comprising a second network, the at least one legacy server operatively connected to the second network, the

VPN extranet gateway operatively connected between the second network and the network.

4. A method for secure legacy enclaves in a Public Key Infrastructure (PKI) comprising:

installing a virtual private network (VPN) extranet gateway between at least one legacy server and a legacy client platform;

attempting access to a legacy application on the at least one legacy server by a user employing legacy client software on the legacy client platform;

requesting a signature certificate of the user by the VPN extranet gateway to authenticate the user;

querying a directory by the VPN extranet gateway after authenticating the user to confirm the user is allowed access to the at least one legacy server; and

establishing a connection between the legacy client software and the legacy application if the user is allowed access to the at least one legacy server.

5. The method according to claim 4, further comprising configuring the VPN extranet gateway with users allowed access to the at least one legacy server after the installing the VPN extranet gateway between the at least one legacy server and the legacy client platform.

6. The method according to claim 4, wherein the directory comprises a database.

7. The method according to claim 4, further comprising requesting a user ID and password from the user by the legacy server after the connection is established between the legacy client software and the legacy application.

8. The method according to claim 4, further comprising requesting a user ID and password from the user by the VPN extranet gateway before the connection is established between the legacy client software and the legacy application.

9. An article comprising a storage medium having instructions stored therein, the instructions when executed causing a processing device to perform:

receiving an attempt to access a legacy application on a legacy server by a user employing legacy client software;

requesting a signature certificate of the user to authenticate the user;

querying a directory to confirm the user is allowed access to the legacy server after authenticating the user; and

establishing a connection between the legacy client software and the legacy application if the user is allowed access to the legacy server.

10. The article according to claim 9, further comprising requesting a user ID and password from the user before the connection is established between the legacy client software and the legacy application.

11. The article according to claim 9, receiving configuration information regarding users allowed access to the at least one legacy server.